

Serial No. 09/754,018

### **Amendments to the Drawings**

The attached replacement sheet(s) of drawings replace(s) the sheets with the corresponding figures. The replacement sheets include the following changes:

*Fig. 6 was changed to correct block 63, which now reads "Internal function" as opposed to "Public function".*

## Remarks

The various parts of the Office Action (and other matters, if any) are discussed below under appropriate headings.

### ***Drawings***

Fig. 6 has been amended to show block 63 as being an "Internal function". Support for the amendment can be found, for example, on page 12, lines 4-17 of the application as filed.

### ***Claim Rejections - 35 USC § 103***

Claims 1, 3 and 6-9 stand rejected under 35 USC §103(a) based on U.S. Patent No. 5,982,887 (*Hirofani*) in view of U.S. Patent No. 6,907,125 (*Oishi*) in further view of Applied Cryptography (*Schneier*), and in further view of U.S. Patent No.6,526,462 (*Elabd*). Further, claims 1, 3 and 6-9 also stand rejected under 35 USC §103(a) based on *Hirofani*, *Schneier* and *Elabd* in view of U.S. Patent No. 5,613,005 (*Murakami*). Withdrawal of the rejections is respectfully requested for at least the following reasons.

Independent claims 1, 3, 6 and 8 have been amended herein to include features of original claim 2, as well as additional features disclosed in the application. Independent claims 1, 3, 6 and 8 now recite a recovered program that includes at least a public function which is to be called from outside of the recovered program and an internal function which is to be called from inside of the recovered program, and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program. Support for this amendment can be found, for example, in original claim 2 and on page 12, lines 4-26.

An objective of the present invention is to provide a control program including a program to be concealed that is implemented partially by hardware and partially by software (see, e.g., pg. 4, Ins. 18-23 of the application). Therefore, even a person who develops very sophisticated software technology cannot decrypt the cryptograph merely by analyzing the control program. Moreover, the method for performing the recovery

processing of the concealed program according to the present invention is superior to that performed within hardware or software alone (see pg. 14, Ins. 1-17).

In particular, according to the method for executing an instruction concealed in the concealed program 317, as shown in Fig. 5B of the present application, the copied program 502 in rewritable memory 105 is recovered as a recovered program 503 using the data scramble circuit 103. Thereafter, the MPU 102 calls a function in the recovered program 503 (see, e.g., pg. 10, ln. 24-pg. 11, ln. 14). As shown in Fig. 6, the recovered program 503 includes a relative address list 60 and a program portion 66. The program portion includes public functions 61 and 62, which are called from outside of the recovered program 503 and internal functions 63, 64 and 65, which are called from inside of the recovered program 503 using relative addresses. The relative address list 60 includes the relative addresses of the public functions 61 and 62. For example, the public functions 61 and 62 are called from the non-concealed program 500, and the public function 61 calls the internal functions 63 and 64 using relative addresses (see, e.g., pg. 11, kn. 32-pg. 12, ln. 26).

Original claims 2 and 5 were rejected as being unpatentable over *Hirofani*, *Schneider* and *Elabd* as applied to claims 1 and 3, respectively, and in further view of *Oaulline* and *Ooi*. None of these references, however, have been found to teach or suggest the features of amended claims 1, 3, 6 and 8. *Oaulline* describes how to create a function (see pg. 133 of *Oaulline*), but has not been found to teach a recovered program recovered from a concealed program that includes at a least a public function which is called from outside of the recovered program and an internal function which is called from inside of the recovered program, and a relative address list indicating a relative address of the at least one public function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

With respect to *Ooi*, an objective is to provide a program counter/relative address calculation system capable of executing an instruction decoding and an operand address calculation in parallel in a pipeline (see col. 2, Ins. 58-66 of *Ooi*). *Ooi* also has not been found to disclose a recovered program recovered from a concealed program that includes at a least a public function which is called from outside of the recovered program and an internal function which is called from inside of the recovered program, and a relative address list indicating a relative address of the at least one public

function in the recovered program, wherein the relative address list is provided at a prescribed location in the recovered program.

*Hirofani* discloses an encrypted program executing apparatus, wherein a decryption process is performed by a CPU executing a decryption program stored in ROM. No mention of a public function called from outside of the recovered program and an internal function called from inside the recovered program has been found in *Hirofani*.

*Oishi* and *Murakami* are both cited for teaching encryption and decryption circuits that correct errors during decryption. No mention of internal or public functions have been found in *Oishi* or *Murakami*.

*Elabd* is cited for teaching circuits can be implemented using a "system on chip" (SOC) design, as opposed to traditional, separate component integrated circuit designs. *Elabd* also has not been found to disclose a public function called from outside of the recovered program and an internal function called from inside the recovered program.

*Schneider* is cited for teaching hardware encryption/decryption can be performed in a hardware circuit. No mention of a public function called from outside of the recovered program and an internal function called from inside the recovered program has been found in *Schneider*.

The cited art has not been found to teach or suggest all the features of amended claims 1, 3, 6 and 8. Accordingly, withdrawal of the rejection of claims 1, 3, 6 and 8 is respectfully requested.

Claims 7 and 9 depend from claims 6 and 8, respectively, and therefore can be distinguished from the cited art for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 7 and 9 is respectfully requested.

Serial No. 09/754,018

**Conclusion**

In view of the foregoing, request is made for timely issuance of a notice of allowance.

Respectfully submitted,

RENNER, OTTO, BOISSELLE & SKLAR, LLP

By /Kenneth W. Fafrak/  
Kenneth W. Fafrak, Reg. No. 50,689

1621 Euclid Avenue  
Nineteenth Floor  
Cleveland, Ohio 44115  
(216) 621-1113

**CERTIFICATE OF MAILING OR FACSIMILE TRANSMISSION UNDER 37 CFR 1.8(a)**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is  
\_\_\_ being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope  
addressed to the Commissioner for Patents address below.

\_\_\_ being transmitted via EFS or via facsimile to (571) 273-8300 (Centralized Facsimile Number) at the U.S.  
Patent and Trademark Office.

☒ submitted on the date shown below using the U.S. Patent Office's Electronic Filing System.

/Kenneth W. Fafrak/

**April 12, 2007**

E:\YY\AMA\PO748US\Reply\_to\_OA\_1\_12\_07.wpd